Judge in FBI Hacking Case Is Unclear on How FBI Hacking Works

6-8 minutes

As criminals continue to protect themselves with encryption and anonymization tech, cops are moving to hacking as an investigatory tool. Over the years, the FBI in particular has launched several campaigns to obtain data from suspects' computers via malware, often using the term "Network Investigative Technique", or NIT, to describe the software being used.

But a problem in some NIT cases is that judges have trouble understanding, even in general terms, what a hacking tool is, what they do, or how they work. To be clear, this isn't to place all blame on judges. Instead, it's arguably a problem stemming from how the Department of Justice and the FBI have framed and referred to NITs in legal documents, meaning that some judges may not fully realise the power and scope of the searches that they authorise.

On Friday, a hearing was held in Seattle dealing with the case of Jay Michaud, a Vancouver, Washington public school administration worker arrested on child pornography charges last year. He was charged after FBI investigators seized Playpen, a Tor hidden service, and then hosted it from their own servers. From here, the FBI deployed a NIT designed to target users of the site and return their real IP address, amongst other technical information.

During the hearing, Judge Robert. J Bryan seemed to not understand how a NIT, or, more broadly, a piece of information-siphoning malware works. This confusion, in part, arose from the language used in NIT warrants and supporting documents. The word "hack," is never used, and neither is "malware" or "exploit," for that matter. Instead, the procedure of malware being downloaded to a target's computer is largely obfuscated in vague terminology.

> "I suppose there is somebody sitting in a cubicle somewhere with a keyboard doing this stuff. I don't know that. It may be they seed the clouds, and the clouds rain information."

"In the normal course of operation, web sites send content to visitors," reads the application for a search warrant as part of Operation Torpedo, when a NIT was deployed on a number of hidden services in 2012.

"A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the web site would augment that content with some additional computer instructions," it continues.

This section also appeared in the Playpen NIT documentation, which Judge Bryan held particular issue with.

"You see, that is the kind of paragraph I don't understand fully," he said during the hearing, pointing to the line that describes how websites send content to visitors, according to a court transcript. "And I am trying to understand."

A hangup also occurred around the misinterpretation of "instructions"—Judge Bryan used the word in the context of a human following a list of instructions, but the warrant refers to computer code as instructions.

Another exchange showed how it can be difficult for judge's to conceptualise where data obtained from malware is sourced from, and where it goes.

"Do the FBI experts have any way to look at the NIT information other than going to the server?" Judge Bryan asked.

"Your Honor, they don't go to the server," Colin Fieman, a federal public defender who is representing Michaud, replied.

"Where do they go? How do they get the information?"

"They get it from Mr. Michaud's computer."

"They don't have his computer."

"That's what the NIT is for," Fieman explained.

This back and forth continues for several pages in the transcript, and testimony around the use of the NIT was also given by FBI Special Agent Daniel Alfin, who worked on identifying suspected Playpen users.

In short, Judge Byran, despite hearing the views of those who took part in the investigation, and having read the briefs submitted by the defense and prosecution several times, could not fully grasp what the NIT was doing.

"If a smart federal judge still has trouble understanding after hours of expert testimony what is actually going on," then the average judge signing warrant applications has little hope of truly understanding what the FBI is proposing, Nate Wessler, staff attorney at the American Civil Liberties Union (ACLU), told Motherboard in a phone interview. (The ACLU has agreed to a protective order for the Michaud case, allowing it access to the sealed filings.)

"It appears in this case, and that's consistent with other cases we've seen elsewhere in the country involving use of malware, the government explanations and warrant applications are quite sparse, and do not fully explain to judges how these technologies works," Wessler added.

Screenshot from court transcripts.

As the hearing continued, Judge Byran said "I suppose there is somebody sitting in a cubicle somewhere with a keyboard doing this stuff. I don't know that. It may be they seed the clouds, and the clouds rain information. I don't know."

There is also the issue of documents arguably not being entirely clear about where the actual search of a computer is going to take place.

In previous warrants, including that of Operation Torpedo, investigators have written that the search will take place within the issuing district, "and elsewhere." In the Playpen case, however, that phrase has been omitted, leaving only the district in which the warrant was signed.

"This search happened on a computer located in Vancouver, Washington," Fieman said in the hearing, referring to his client's computer. "The warrant on its face is limited to persons and property in the Eastern District of Virginia."

Keith Becker, an attorney from the Department of Justice, said in the hearing that the warrant "clearly requested the authorities to deploy to computers wherever located."

Magistrate Judge Theresa C. Buchanan in the Eastern District of Virginia, who signed the NIT warrant for the Playpen case, was not available for comment. "Judge Buchanan does not respond to media inquiries," Christian Schreiber, a law clerk to the judge, told Motherboard in an email. The Department of Justice did not respond to a request for comment.

"When it comes to this kind of secret and hard to understand technological search, the government holds all the cards, and it is crucial that the government be very careful to explain itself fully and accurately," Wessler added.